



TITLE:

# Nombres de classes dans certaines extensions infinies(Algebraic Number Theory)

AUTHOR(S):

Gillard, par R.

---

CITATION:

Gillard, par R.. Nombres de classes dans certaines extensions infinies(Algebraic Number Theory). 数理解析研究所講究録 1987, 603: 60-71

ISSUE DATE:

1987-01

URL:

<http://hdl.handle.net/2433/99656>

RIGHT:

## Nombres de classes

dans certaines extensions infinies.

par R. Gillard (Grenoble)

Le but de cette conférence <sup>†</sup> est de discuter comment le théorème de Washington, prolongé par Friedman, (cf. [W1] et [F]) peut se transposer dans le cadre des extensions abéliennes d'un corps quadratique imaginaire. Pour plus de détails, je renvoie à mon article [Gi3].

Rappelons brièvement la situation cyclotomique. Pour  $l$  un nombre premier, notons  $\mathbf{Q}_{l^\infty}$  l'unique  $\mathbf{Z}_l$ -extension de  $\mathbf{Q}$ ; elle est contenue dans la réunion des corps cyclotomiques  $\mathbf{Q}(\zeta_{l^n})$ , pour  $n$  dans  $\mathbf{N}$ ,  $\zeta_{l^n}$  racine de 1 d'ordre  $l^n$ . Soient pour  $s$  entier  $l_1, \dots, l_s$  des nombres premiers distincts fixés; posons  $\Lambda := \prod l_i$  et  $\Lambda^n := \prod l_i^{n_i}$ , si  $\mathbf{n} := (n_1, \dots, n_s)$ . On note  $\mathbf{Q}_{\Lambda^\infty}$  l'extension composée des  $\mathbf{Q}_{l_i^\infty}$ . Pour  $F/\mathbf{Q}$  une extension abélienne, notons  $F_{\Lambda^\infty}$  l'extension composée  $F \cdot \mathbf{Q}_{\Lambda^\infty}$  et  $F_{\Lambda^n}$ ,  $\mathbf{n}$  comme ci-dessus, la sous-extension de  $F_{\Lambda^\infty}/F$  de degré  $\Lambda^n$ . Fixons un nombre premier  $p$  et notons  $e(\mathbf{n})$  l'exposant de  $p$  dans le nombre de classes de  $F_{\Lambda^n}$ . D'après [F], on a:

0.1. THÉOREME. — Avec les notations précédentes, fixons  $\Lambda$  et  $F$ : si  $p$  ne divise pas  $\Lambda$ , l'exposant  $e(\mathbf{n})$  est borné lorsque  $\mathbf{n}$  parcourt  $\mathbf{N}^s$ .

Ce théorème redonne celui de [W1] lorsque  $s = 1$ . En utilisant le théorème de Ferrero-Washington, [FW] ( $\mu = 0$ ; c'est le cas  $s = 1$  dans 0.2), Friedman en déduit:

0.2. THÉOREME. — Avec les notations précédentes, si  $p$  est égal à  $l_1$ , il existe des entiers  $\lambda \geq 0, \nu \in \mathbf{Z}, m_1, \dots, m_s \in \mathbf{N}$  tels que pour tout  $\mathbf{n} = (n_1, \dots, n_s)$  vérifiant  $n_1 \geq m_1, \dots, n_s \geq m_s$ , on ait:

$$(0.2.1) \quad e(\mathbf{n}) = \lambda \cdot n_1 + \nu.$$

De plus la limite projective naturelle des groupes de classes des extensions  $F_{\Lambda^n}$  pour  $\mathbf{n} \in \mathbf{N}^s$  est isomorphe à  $(\mathbf{Z}_p)^\lambda$ .

<sup>†</sup> Je remercie sincèrement la fondation Taniguchi qui l'a permise

## 1. Résultats.

**1.0.** — Plaçons nous maintenant dans la situation "elliptique" en choisissant un corps quadratique imaginaire  $K$  d'anneau des entiers  $R$ . Pour chaque idéal premier  $\underline{l}$  de  $R$  soit  $R_{\underline{l}}$  le complété de  $R$  en  $\underline{l}$  et  $K_{\underline{l}\infty}$  l'unique  $R_{\underline{l}}$ -extension de  $K$  non ramifiée en dehors de  $\underline{l}$ ; si  $\underline{l}$  diffère de son conjugué  $\underline{l}'$ , notre  $K_{\underline{l}\infty}$  est la  $\mathbf{Z}_{\underline{l}}$ -extension de  $K$  non ramifiée en dehors de  $\underline{l}$ ; si  $\underline{l} = \underline{l}'$ , c'est la  $\mathbf{Z}_{\underline{l}} \times \mathbf{Z}_{\underline{l}}$  extension de  $K$ . Soient, pour  $s$  entier, des idéaux premiers distincts  $\underline{l}_1, \dots, \underline{l}_s$  de  $R$  et  $\Lambda$  leur produit. Pour  $\mathbf{n} := (n_1, \dots, n_s)$ , posons  $\Lambda^{\mathbf{n}} := \prod \underline{l}_i^{n_i}$ . Soit  $R_{\Lambda}$  le complété  $\Lambda$ -adique de  $R$ : il s'identifie au produit des  $R_{\underline{l}_i}$ ; notons  $K_{\Lambda\infty}$  la composée des extensions  $K_{\underline{l}_i\infty}$ ; on a  $\text{Gal}(K_{\Lambda\infty}/K) \simeq R_{\Lambda}$ .

Soient  $F$  une extension abélienne de  $K$  et  $F_{\Lambda\infty}$  l'extension composée  $F.K_{\Lambda\infty}$ . Choisissons maintenant un nombre premier  $p$  et un diviseur premier de  $\bar{p}$  dans  $R$ ; on suppose que

**HYPOTHÈSE.** —  $p$  est  $\neq 2$  ou  $3$  et est non ramifié dans  $K/\mathbf{Q}$ .

Pour chaque extension  $L/K$  notons  $M(L)/L$  la plus grande  $p$ -extension abélienne non ramifiée en dehors de  $\bar{p}$ . Soit  $X(L)_{\tau}$  la partie de torsion de  $X(L) := \text{Gal}(M(L)/L)$  et  $x(L)$  l'exposant de  $p$  dans son ordre. On peut se demander:

**QUESTION.** — *Quelles sont les conditions sur  $F$  et  $\Lambda$  qui assurent que*  
**(1.0.1)** *le nombre  $x(L)$  reste borné lorsque  $F$  parcourt l'ensemble des sous-extensions de  $F_{\Lambda\infty}/F$ .*

Le résultat suivant incite à la prudence:

**1.1. THÉORÈME.** — *Soit  $l \neq p$  un nombre premier; prenons  $\Lambda = (l)$ . Considérons  $H^{(p)}$  la plus grande  $p$ -extension non ramifiée de  $K$ : elle possède une infinité d'extensions cycliques  $F/H^{(p)}$  de degré  $p$ , abéliennes sur  $K$ , et ne vérifiant pas (1.0.1).*

**Démonstration.** — (esquisse: cf. aussi [I1]) On considère les extensions

$F/H^{(p)}$  comme ci-dessus qui sont ramifiées en suffisamment d'idéaux premiers au dessus de nombres premiers inertes dans  $K$ : on constate que ces idéaux se décomposent totalement dans une  $\mathbf{Z}_l$ -sous-extension de  $K_{\Lambda^\infty}$ . On applique alors une formule des classes invariantes (similaire à celle de [Gr]) pour les extensions  $L/L \cap H_{\Lambda^\infty}^{(p)}$ . On a remplacé  $K$  par  $H^{(p)}$  pour assurer l'existence de tels  $F$ .  $\square$

Notre résultat essentiel donne une condition suffisante pour avoir (1.0.1):

**1.2. THÉORÈME.** — *On suppose que  $p$  ne divise pas  $\Lambda$ . Avec les notations de 1.0, et l'hypothèse sur  $p$ , si l'extension  $F_{\Lambda^\infty}/F$  est pro-cyclique, alors (1.0.1) est vraie.*

Imposer que  $F_{\Lambda^\infty}/F$  soit pro-cyclique revient à demander que l'idéal  $\Lambda$  soit premier à son conjugué: les idéaux  $\underline{l}_i$  sont alors de degré 1 et ne sont pas conjugués deux à deux.

*Démonstration.* — On déduit 1.2 du théorème 3.2.4 ci dessous et de critères de Kummer (cf. [Gi2] et [R2] ou pour plus de détails [Gi3]).  $\square$

En suivant la méthode de Friedman et en s'appuyant sur le résultat  $\mu = 0$  de [Gi2], on déduit assez facilement de 1.2 l'analogue de 0.2:

**1.3 THÉORÈME.** — *On suppose l'extension  $F_{\Lambda^\infty}/F$  pro-cyclique et on note  $F_{\Lambda^n}$  la sous-extension de degré  $N(\Lambda^n)$ . Alors si  $\underline{p} = \underline{l}_1$  et si  $p$  vérifie l'hypothèse de (1.0), la limite projective naturelle des  $X(F_{\Lambda^n})$  est un  $\mathbf{Z}_p$ -module libre de rang fini. En notant  $\lambda$  son rang, on trouve qu'il existe des entiers  $\nu \in \mathbf{Z}$  et  $m_1, \dots, m_s \in \mathbf{Z}$  tels que*

$$x(F_{\Lambda^n}) = \lambda.n_1 + \nu,$$

*pour  $\mathbf{n}$  dans  $\mathbf{N}^s$  vérifiant  $n_1 \geq m_1, \dots, n_s \geq m_s$ .*

*Démonstration.* — Si  $L/K$  est une extension infinie, posons

$$M(L) := \bigcup M(L'), \quad X_r(L) := \varprojlim X(L')_r = \text{Gal}(M(L)/L_{\underline{p}^\infty}),$$

où dans la réunion et la limite projective  $L'$  parcourt l'ensemble des sous-extensions finies de  $L$ . Notons  $\Lambda_0$  le produit de  $\underline{l}_i$  pour  $i \geq 2$  et  $F_n$  (resp.  $F'_n$ ) la sous

extension de degré  $p^n$  de  $F_{\underline{p}^\infty}/F$  (resp.  $F_{\Lambda^\infty}/F_{\Lambda_0^\infty}$ ). On remarque tout d'abord que le théorème 1.2 implique la finitude de  $X_\tau(F'_n)$ , et on en déduit que  $X_\tau(F_{\Lambda^\infty})$  est un  $\mathbf{Z}_p[[T]]$ -module de torsion (on a identifié  $T - 1$  à un générateur fixé de  $\text{Gal}(F_{\Lambda^\infty}/F_{\Lambda_0^\infty})$ ). Comme dans [F], on ramène facilement son étude à celle de  $X_\tau(L)$  pour un  $L$  compris entre  $F_{\underline{p}^\infty}$  et  $F_{\Lambda^\infty}$  et  $[L : F_{\underline{p}^\infty}]$  fini. On vérifie que  $L = F_{\underline{p}^\infty}'''$  pour une extension  $F'''$  convenable. La formule du début se déduit de la théorie d'Iwasawa appliquée à  $F'''$  (cf. [W2] 13.5), compte tenu du théorème 3.4 ( $\mu = 0$ ) de [Gi2].  $\square$

**1.4.** — Les énoncés précédents sont encore valides en remplaçant  $X(L)$  par le  $p$ -groupe des classes de  $L$ , cela en est une conséquence facile si  $p$  est décomposé; pour  $p$  inerte c'est un peu plus délicat.

## 2. Un résultat d'indépendance algébrique.

Comme dans [Gi2], [S1] et [S2], la démonstration repose sur un résultat d'indépendance algébrique. On prend  $R$  et  $\Lambda$  comme en 1.0.

**2.1.** — Soit  $E$  une courbe elliptique à multiplications complexes par  $R$  définie sur un corps  $k$  de caractéristique première à  $\Lambda$ . Notons  $E[\Lambda^\infty]$  les points de  $E$  à valeurs dans une clôture algébrique  $\bar{k}$  de  $k$  et annulés par une puissance (variable) de  $\Lambda$ .

**2.2. PROPOSITION.** — Soit  $W$  une partie infinie de  $E[\Lambda^\infty]$  et  $\beta_1, \dots, \beta_s$  des éléments de  $R_\Lambda$  linéairement indépendants sur  $R$ ; alors les points  $P(w)$  de composantes  $\beta_i.w$ , pour  $w$  dans  $W$ , dans le produit  $E^s$  de  $s$  copies de  $E$ , forment un ensemble dense pour la topologie de Zariski.

*Démonstration.* — La fermeture de l'ensemble des  $P(w)$  est une sous-variété abélienne de  $E^s$ . Si ce n'était pas  $E^s$  lui-même, les  $P(w)$  seraient dans le noyau d'un morphisme surjectif de variétés abéliennes  $E^s \rightarrow E$ , ce qui fournirait une relation de dépendance entre les  $\beta_i$ .  $\square$

2.3. COROLLAIRE. — Soient  $W$  une partie infinie de  $E(\Lambda^\infty)$  et des  $\delta_j$ , pour  $j = 1, \dots, m$  dans  $R_\Lambda^*$ , ainsi que des fonctions rationnelles  $f_j$  sur  $E$ . Si les  $\delta_j$  représentent des classes distinctes dans le quotient  $R_\Lambda^*/R_\Lambda^* \cap R$  et si la somme  $\sum f_j \circ \delta_j$  est nulle sur  $W$ , alors les fonctions  $f_j$  sont constantes.

Démonstration. — Il suffit de reprendre celle de [S1].  $\square$

### 3. Etude d'une famille infinie de nombres de Bernoulli-Hurwitz.

3.1. Notations complémentaires. — Soient  $K = \mathbb{Q}(\sqrt{d})$  notre corps quadratique imaginaire ( $d < 0$  est le discriminant), et  $\underline{p}$  comme en 1.0; on identifie les nombres algébriques dans  $\mathbb{C}$  et  $\mathbb{C}_p$  (complété d'une clôture algébrique  $\overline{\mathbb{Q}_p}$  de  $\mathbb{Q}_p$ ) à l'aide d'inclusions  $\overline{\mathbb{Q}} \subset \mathbb{C}$  et  $\overline{\mathbb{Q}} \subset \mathbb{C}_p$  fixées: ceci définit un prolongement  $v$  à  $\overline{\mathbb{Q}}$  de la valuation  $\underline{p}$ -adique de  $K$  compatible avec la valuation de  $\mathbb{C}_p$  que l'on note aussi  $v$  et que l'on normalise par  $v(p) = 1$ . Pour toute extension  $L$  de  $\mathbb{Q}$  ou  $\mathbb{Q}_p$ , on note  $R(L)$  son anneau d'entiers. On note  $\underline{p}$  l'idéal maximal de  $R(\mathbb{C}_p)$ . On pose  $R := R(K)$ .

Soit  $E$  une courbe elliptique admettant  $R$  comme anneau d'endomorphismes. Pour  $a \in R$ , on note  $[a]$  l'endomorphisme correspondant. On suppose que  $E$  est définie sur  $H$ , le corps de Hilbert de  $K$ , et a bonne réduction en les diviseurs premiers de  $\underline{p}$ .

Pour  $\mathcal{L} := R.\Omega$ , un réseau convenable, on a le paramétrage de Weierstrass

$$(3.1.1) \quad z \rightarrow (X, Y) := (\wp(z, \mathcal{L}), \wp'(z, \mathcal{L})) .$$

Pour  $\lambda$  un point de torsion de  $E$ , on note  $z(\lambda) \in \mathbb{C}$  un nombre complexe le représentant par (3.1.1). Comme toujours, on utilise une fonction  $\theta$ ,  $\theta(z, \mathcal{L})$  que l'on tord avec une combinaison linéaire d'idéaux de  $R$ ,  $\alpha = \sum \alpha(a) a$  telle que

$$(3.1.2) \quad \alpha(a) \in \mathbb{Z}, \sum \alpha(a) = \sum \alpha(a).N(a) = 0 ,$$

où  $N(a)$  est la norme de  $a$ , pour obtenir une fonction elliptique  $F_\alpha$ , rationnelle sur  $H$ : on définit  $F_\alpha$  sur  $\mathbb{C}$  par sa composée  $\Theta(z, \alpha)$  avec (3.1.1):

$$(3.1.3) \quad \Theta(z, \alpha) := \prod_a \prod_\lambda (\wp(z, \mathcal{L}) - \wp(z(\lambda), \mathcal{L}))^{12.\alpha(a)} ,$$

où dans le produit interne  $\lambda$  parcourt un système de représentants  $\neq 0$  de la  $\mathfrak{a}$ -torsion de  $E$  modulo l'action de  $\pm 1$ . On a

$$(3.1.4) \quad F_\alpha \circ [a] = F_{\alpha(a)} .$$

Soit  $D$  la dérivation invariante  $\frac{d}{dz}$  sur  $E$ : elle est rationnelle sur  $H$  car elle s'écrit encore  $D = Y dX$ ; ainsi  $D \log \Theta(z, \alpha)$  est la fonction rationnelle sur  $E$ :

$$(3.1.5) \quad D \log F_\alpha = \sum_{\mathfrak{a}} \sum_{\lambda} 12 \cdot \alpha(\mathfrak{a}) \frac{Y}{X - X(\lambda)} .$$

Soit  $\mathfrak{g}$  un idéal de  $R$  et choisissons un générateur sur  $R$ ,  $\rho_{\mathfrak{g}}$  de la  $\mathfrak{g}$ -torsion  $E(\mathfrak{g})$  de  $E$ . Si  $\mathfrak{g}$  est premier à  $\Lambda$ , on prend  $\rho_{\mathfrak{g}\Lambda^n} = \rho_{\mathfrak{g}} + \rho_{\Lambda^n}$ .

On note  $Cl(\mathfrak{g})$  (resp.  $H_{\mathfrak{g}}$ ) le groupe (resp. le corps) de classes de rayon  $\mathfrak{g}$ ,  $\mu(\mathfrak{g})$  le groupe des racines de 1 dans  $K$  congrues à 1 modulo  $\mathfrak{g}$  et  $e(\mathfrak{g})$  son ordre. Le nombre  $\Theta(\rho_{\mathfrak{g}}, \alpha)$  est une unité elliptique; son image par l'automorphisme d'Artin  $[b, H_{\mathfrak{g}}/K]$  est donné, cf. [R1] §4.2 prop. 9 cor., par:

$$(3.1.6) \quad [b, H_{\mathfrak{g}}/K] \Theta(\rho_{\mathfrak{g}}, \alpha) = \Theta(\rho_{\mathfrak{g}}, \alpha b) .$$

Soit  $\nu$  un caractère de Dirichlet de  $K$  de conducteur  $\mathfrak{g}$ : par la loi de réciprocité, on l'identifiera à un caractère de  $\text{Gal}(H_{\mathfrak{g}}/K)$  ou même de  $\text{Gal}((H_{\mathfrak{g}})_{\Lambda^\infty}/K)$ . Si  $\nu$  est modérément ramifié en  $\underline{p}$ , son conducteur est de la forme  $\mathfrak{g}$  ou  $\mathfrak{g}\underline{p}$  pour  $\mathfrak{g}$  premier à  $\underline{p}$ . On voit facilement qu'il existe un entier  $n = n(\nu) \in [1, N(\underline{p}) - 1]$  tel que pour  $a$  dans  $R$  congru à 1 modulo  $\mathfrak{g}$ , on ait:

$$(3.1.7) \quad \nu((a)) \equiv a^n \pmod{\underline{p}} .$$

D'après (3.1.7),  $n$  est divisible par  $e(\mathfrak{g})$ .

Pour  $k \in \mathbb{N}$ , et  $k \geq 0$ , on note  $LF_\alpha^{(k)}$  la fonction rationnelle de  $E/H$  définie par la fonction complexe  $\frac{D^k}{(k-1)!} \log F_\alpha$ . De (3.1.4), on déduit

$$(3.1.8) \quad LF_{\alpha(b)}^{(k)} = b^k LF_\alpha^{(k)} \circ [b] .$$

Remarquons l'intégralité de  $LF_\alpha^{(k)}$  en  $\underline{p}$  pour  $k \in [1, N(\underline{p}) - 1]$ , cf. [K] si  $\underline{p}$  est inerte dans  $K$ . Si le conducteur de  $\nu$  est  $\mathfrak{g}$  ou  $\mathfrak{g}\underline{p}$ , on déduit de (3.1.7) que pour  $n = n(\nu)$ ,

$$(3.1.9) \quad \nu^{-1}(b) LF_{\alpha b}^{(n)}(\rho_{\mathfrak{g}}) \equiv LF_\alpha^{(n)}(\rho_{\mathfrak{g}}) \pmod{\underline{p}} ,$$

si  $\mathbf{b}$  est de la forme  $(b)$  avec  $b \equiv 1 \pmod{g}$ . On peut par ailleurs exprimer ces nombres au moyen des valeurs spéciales de séries d'Eisenstein ajustées (cf. [Gi2] 2.4.4)

$$(3.1.10) \quad LF_{\alpha}^{(n)}(\rho_g) = 12(-1)^{n-1} \sum_{\mathbf{a}} \alpha(\mathbf{a}) E_n^*(\rho_g, \mathbf{a}^{-1} \mathcal{L}).$$

**3.2. Nombres de Bernoulli-Hurwitz.** — Soit  $\nu$  un caractère de Dirichlet modérément ramifié en  $\underline{p}$ : on peut écrire la somme:

$$(3.2.1) \quad B_{\alpha}(\nu) := \sum \nu^{-1}(\mathbf{b}) LF_{\alpha \mathbf{b}}^{(n)}(\rho_g).$$

où  $\mathbf{b}$  parcourt un système de représentants de  $Cl(\mathbf{g})$  premiers à  $\underline{p}$  et  $n = n(\nu)$ ;  $B_{\alpha}(\nu) \pmod{\underline{p}}$  est indépendant du système choisi, cf. (3.1.9). Dans le cas où  $n = N(\underline{p}) - 1$  (cas non ramifié en  $\underline{p}$ ), on utilise aussi les nombres

$$(3.2.2) \quad b_{\alpha}(\nu) := \sum \nu^{-1}(\mathbf{b}) \log_p F_{\alpha \mathbf{b}}(\rho_g),$$

où  $\log_p$  est le logarithme calculé dans  $\overline{\mathbb{Q}}_p$ , relié à  $B_{\alpha}(\nu)$  par une congruence.

**3.2.3. Conditions sur  $\alpha$ .** — On suppose que les idéaux  $\mathbf{a}$  tels que  $\alpha(\mathbf{a}) \neq 0$  sont premiers à  $6pg\Lambda$ . On suppose aussi que  $\alpha$  n'a pas tous ses coefficients  $\alpha(\mathbf{a})$  divisibles par  $p$ .

Notons  $\text{Gal}(K_{\Lambda^{\infty}}/K)^*$  le groupe des caractères de  $\text{Gal}(K_{\Lambda^{\infty}}/K)$ . Notre résultat principal est le suivant:

**3.2.4. THÉOREME.** — Si  $\Lambda$  et  $\Lambda'$  sont premiers entre eux et premiers à  $p$  et si  $\chi$  est un caractère de Dirichlet modérément ramifié en  $\underline{p}$ , l'ensemble

$$\mathcal{M}(\chi) := \{\varphi \in \text{Gal}(K_{\Lambda^{\infty}}/K)^* \mid B_{\alpha}(\varphi\chi) \equiv 0 \pmod{\underline{p}}\}$$

est fini.

La proposition suivante joue un rôle capital:

**3.2.5. PROPOSITION.** — Un automorphisme  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/H)$  agit sur le nombre algébrique  $B_{\alpha}(\nu)$  en vérifiant la congruence:

$$\sigma B_{\alpha}(\nu) = c(\sigma) B_{\alpha}(\sigma\nu) \pmod{\underline{p}},$$



où  $\sigma\nu$  est le caractère déduit de  $\nu$  par action sur ses valeurs, et  $c(\sigma)$  est une unité dans  $\overline{\mathbb{Q}_p}$ .  $\square$

**3.3. Trace du caractère  $\nu = \varphi\chi$ .** — Choisissons deux entiers  $N$  et  $M$  ayant les mêmes facteurs premiers que  $\Lambda$ , avec  $N \geq M$  et assez grands pour que

$$(3.3.1) \quad \text{Gal}(H(\mu_N)/H(\mu_M)) \simeq \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}(\mu_M)),$$

et notons  $Tr_{N/M}$  l'opérateur  $\sum \sigma$  où  $\sigma$  parcourt  $\text{Gal}(H(\mu_N)/H(\mu_M))$ .

**3.3.2. LEMME.** — Si  $\nu$  est un caractère d'ordre  $M$ , on a:

$$Tr_{N/M}(\nu(\mathbf{b})) = \begin{cases} [\mathbb{Q}(\mu_N) : \mathbb{Q}(\mu_M)] \nu(\mathbf{b}) & \text{si } \nu(\mathbf{b})^M = 1, \\ 0 & \text{sinon.} \end{cases}$$

Ce lemme évident est important car suivant l'astuce de [W1], il permet de réduire des caractères de Dirichlet à des fonctions caractéristiques pour des sous-ensembles de  $Cl(\mathfrak{g}\Lambda^n)$ .

Voici un premier exemple d'utilisation. Notons  $B'_\alpha(\nu)$  le nombre défini comme  $B_\alpha(\nu)$  mais en restreignant la sommation aux idéaux  $\mathbf{b}$  tels que

$$(3.3.3) \quad [\mathbf{b}, H \cap K_{\Lambda^\infty}/K] = 1;$$

comme en (3.2.5), on a:

$$(3.3.4) \quad \sigma B'_\alpha(\nu) \equiv c(\sigma) B'_\alpha(\sigma\nu) \pmod{\underline{p}}.$$

**3.3.5. PROPOSITION.** — Pour que  $M(\chi)$  soit fini, il suffit qu'il en soit de même pour

$$M'(\chi) := \{\varphi \in \text{Gal}(K_{\Lambda^\infty}/K)^* \mid B'_\alpha(\varphi\chi) \equiv 0 \pmod{\underline{p}}\}$$

*Démonstration.* — En appliquant 3.3.2, on déduit de la congruence d'un  $B_\alpha(\varphi\chi)$  des congruences analogues portant sur des sommes analogues où  $\mathbf{b}$  parcourt un système des représentants de  $Cl(\mathfrak{g}\Lambda^n)$  (où  $\mathfrak{g}\Lambda^n$  est la partie première à  $\underline{p}$  du conducteur de  $\varphi\chi$ ) tels que  $\mathbf{b}$  induise l'identité sur  $K_{(M)}$  (on désigne par  $K_{(M)}$  la sous-extension de degré  $M$  de  $K_{\Lambda^\infty}/K$  et on choisit l'ordre  $N$  de  $\varphi\chi$

et  $M$  assez grands). On termine en sommant sur un système de représentants de  $\text{Gal}(K_{(M)}/K_{\Lambda^\infty} \cap H)$ .  $\square$

**3.4. Comment  $B'_\alpha(\varphi\chi)$  dépend de  $\varphi$ .** — Le passage de  $B_\alpha(\varphi\chi)$  à  $B'_\alpha(\varphi\chi)$  va nous permettre d'isoler  $\varphi$  dans les sommes. Posons

$$\Lambda^{(n)} = \text{pgcd}(\Lambda, 2) \Lambda^n \Lambda.$$

On suppose maintenant que  $\varphi$  est de conducteur exactement  $\Lambda^{(n)}$  et que le conducteur de  $\chi$  divise  $\mathfrak{g}\Lambda^{(0)}$ : ceci est possible par une translation éventuelle sur  $\mathcal{M}'(\chi)$ . On peut prendre comme système de représentants de  $Cl(\mathfrak{g}\Lambda^{(n)})$  le système des

$$(3.4.1) \quad \mathbf{b} = \mathbf{c}.i(x),$$

où  $\mathbf{c}$  parcourt un système de représentants de  $Cl(\mathfrak{g}\Lambda^{(0)})$ ; si  $x$  appartient à  $1 + \Lambda^{(0)}$ , on définit  $i(x)$  comme étant un idéal  $(x')$  avec  $x' \equiv 1 \pmod{\mathfrak{g}\Lambda^{(0)}}$  et  $x' \equiv x \pmod{\Lambda^{(n)}}$ : sa classe dans  $Cl(\mathfrak{g}\Lambda^{(n)})$  est bien définie. On écrit simplement  $\varphi(x)$  pour  $\varphi(i(x))$ . On observe que  $n(\varphi\chi) = n(\chi)$  donc est indépendant de  $\varphi$ . Pour  $\mathbf{b}$  vérifiant (3.3.3), il existe un  $\beta$  unique dans  $1 + \Lambda^{(0)}$  tel que pour tout  $\varphi$  dans  $\text{Gal}(K_{\Lambda^\infty}/K)^*$ , on ait:

$$(3.4.2) \quad \varphi(\mathbf{b}) = \varphi(\beta).$$

Bien sur si  $\mathbf{b} = \mathbf{c}.i(x)$ , on doit prendre  $\beta = \gamma.x$  avec  $\gamma = \gamma(\mathbf{c})$  défini par la condition analogue à 3.4.2.

Après quelques calculs, on obtient:

$$(3.4.1) \quad B'_\alpha(\varphi\chi) = \sum_z \varphi^{-1}(z) \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c}) L F_{\alpha\mathbf{c}}^{(n)}(\rho_{\mathbf{g}} + z \gamma^{-1} \rho_{\Lambda^{(n)}}),$$

où  $z$  parcourt  $1 + \Lambda^{(0)}/1 + \Lambda^{(n)}$  et  $\mathbf{c}$  un ensemble  $\mathcal{R}$  d'idéaux en bijection par  $\mathbf{c} \rightarrow [\mathbf{c}, H_{\mathfrak{g}\Lambda^{(0)}}/K]$  avec  $\text{Gal}(H_{\mathfrak{g}\Lambda^{(0)}}/H \cap K_\infty)$ .

**3.5. Transformation de Fourier.** — Pour  $\rho$  un point de torsion annulé par  $\Lambda^{(n)}$ , on introduit le caractère *additif* sur  $R$ :

$$(3.5.1) \quad \lambda_\rho(a) := \exp 2\pi i \text{Tr}(a \frac{z(\rho)}{\Omega\sqrt{d}}).$$

Si  $\rho$  est primitif, on a ainsi une dualité sur  $R/\Lambda^{(\mathbf{n})}$  définie par  $(x, y) \rightarrow \lambda_\rho(x, y)$ . Pour  $f$  fonction sur  $R/\Lambda^{(\mathbf{n})}$ , on peut introduire sa transformée de Fourier

$$(3.5.2) \quad \mathcal{F}_\rho(f)(y) := \sum_x \lambda_\rho(x, y) f(x),$$

somme sur  $R/\Lambda^{(\mathbf{n})}$ .

Soit  $\varphi \in \text{Gal}(K_{\Lambda^\infty}/K)^*$ , un caractère de conducteur  $\Lambda^{(\mathbf{n})}$ . Choisissons deux éléments  $\mathbf{n}$  et  $\mathbf{m}$  de  $\mathbb{N}^s$  assez gros (i.e. toutes leurs composantes sont assez grosses): les entiers  $N := N(\Lambda^{(\mathbf{n})})$  et  $M := N(\Lambda^{(\mathbf{m})})$  vérifient la condition (3.3.1). On a le résultat suivant qui nous débarrassera de  $\varphi$ :

3.5.3. PROPOSITION. — Supposons que  $\mathcal{M}'(\chi)$  contienne un caractère  $\varphi$  de conducteur  $\Lambda^{(\mathbf{n})}$ , alors le point de torsion  $\rho_{\Lambda^{(\mathbf{n})}}$  vérifie

$$\sum_\varepsilon \lambda_\varepsilon(1) \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c}) LF_{\alpha\mathbf{c}}^{(\mathbf{n})}(\gamma^{-1}\rho_{\Lambda^{(\mathbf{n})}} + \gamma^{-1}\varepsilon + \rho_{\mathbf{g}}) \equiv 0 \pmod{\bar{p}},$$

où dans la somme  $\varepsilon$  parcourt  $E[\Lambda^{(\mathbf{m})}]$ .

Enonçons quelques lemmes utiles pour la démonstration de 3.5.3.

3.5.4. LEMME. — Si  $\varphi \in \text{Gal}(K_{\Lambda^\infty}/K)^*$  est un caractère de conducteur  $\Lambda^{(\mathbf{n})}$ , il existe un point  $\omega$  de  $\Lambda^{(\mathbf{n})}$ -torsion, primitif, tel que

$$\varphi(1 + T) = \lambda_\omega(T);$$

pour tout  $T$  dans  $\Lambda^{(\mathbf{n}-\mathbf{m})}$ .  $\square$

En fait quitte à remplacer  $\varphi$  par un conjugué, on peut même prendre  $\omega = -\rho_{\Lambda^{(\mathbf{n})}}$  dans 3.5.4. C'est dans le résultat suivant que l'hypothèse que  $\Lambda$  et  $\Lambda'$  sont premiers entre eux s'avère indispensable car elle permet d'exprimer le noyau de  $\varphi^{\mathbf{m}}$  dans  $R_\Lambda^*$  et d'appliquer 3.3.2.

3.5.5. LEMME. — Si  $x_0 \in 1 + \Lambda^{\mathbf{m}}$  et si  $x$  dans  $x_0 \eta (1 + \Lambda^{(\mathbf{n}-\mathbf{m})})$ , avec  $\eta \in \mu(R_\Lambda)$  le groupe des racines de 1 dans  $R_\Lambda$ , on a

$$\text{Tr}_{N/M} \varphi(x/x_0) = [\mathbb{Q}(\mu_N) : \mathbb{Q}(\mu_M)] \lambda_\omega\left(\frac{x}{\eta} - x_0\right).$$

C'est 0 si  $x$  est dans  $R_\Lambda$  mais pas dans  $x_0 \mu(R_\Lambda) (1 + \Lambda^{(\mathbf{n}-\mathbf{m})})$ .  $\square$

**3.6. Démonstration de 3.5.3. (esquisse). —** Posons

$$(3.6.1) \quad G(z) := \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c}) \, LF_{\alpha \mathbf{c}}^{(n)}(z\gamma^{-1}\rho_{\Lambda^{(n)}} + \rho_{\mathbf{g}}) .$$

Partant de (3.4.5), en utilisant (3.3.5), on obtient

$$(3.6.2) \quad \sum_z \sigma\varphi^{-1}(z) \, G(z) \equiv 0 \pmod{\underline{p}} .$$

pour  $\sigma$  dans  $\text{Gal}(H(\mu_N)/H(\mu_M))$ . Multipliant le membre de gauche de (3.6.2) par  $\sum_x \lambda_{\rho}(x) \, \sigma\varphi(x)$  (somme sur un système de représentants de  $R/\Lambda^{(n)}$ ; on a posé  $\rho = \rho_{\Lambda^{(n)}}$ ) et remplaçons  $x$  par  $xz$  dans la sommation: nous faisons apparaître  $\mathcal{F}_{\rho}(\sigma\varphi)$ . La proposition s'obtient en faisant une combinaison linéaire astucieuse  $g$  des fonctions  $\sigma\varphi$  pour avoir une fonction  $\mathcal{F}_{\rho}(g)$  très simple, en utilisant 3.5.5.  $\square$

**3.7. Démonstration de 3.2.4. —** Nous allons utiliser le résultat du §2, mais auparavant il nous (encore!) transformer la congruence de 3.5.3. Posons  $\mathbf{c} = \mathbf{b} \cdot (x)$  où  $b$  parcourt un ensemble  $\mathcal{R}_1$  d'idéaux de  $R$  premiers à  $\Lambda^{(0)}$ , ensemble en bijection par  $\mathbf{b} \rightarrow [\mathbf{b}, H_{\Lambda^{(0)}}/H_{\Lambda^{(0)}} \cap K_{\Lambda^{\infty}}]$  avec  $\text{Gal}(H_{\Lambda^{(0)}}/H_{\Lambda^{(0)}} \cap K_{\Lambda^{\infty}}) \dagger$  et où  $x$  parcourt un système de représentants  $\mathcal{R}_2$  tous congrus à 1 mod  $\Lambda^{(0)}$  de  $(R/\mathfrak{g})^*$ . Ainsi les nombres  $\beta$  et  $\gamma$  associés à  $\mathbf{b}$  et à  $\mathbf{c}$  par (3.4.4) vérifient  $\gamma = \beta \cdot x$ . En utilisant 3.1.8, la congruence de 3.5.3 s'écrit donc

$$(3.7.1) \quad \sum_{\mathbf{b} \in \mathcal{R}_1} \chi^{-1}(\mathbf{b}) \, G_{\mathbf{b}}(\beta^{-1} \cdot \rho_{\Lambda^{(n)}}) \equiv 0 \pmod{\underline{p}} .$$

où  $G_{\mathbf{b}}$  est la fonction rationnelle sur  $E$ :

$$(3.7.2) \quad G_{\mathbf{b}}(P) := \sum_{x \in \mathcal{R}_2} \sum_{\varepsilon \in E[\Lambda^m]} \lambda_{\varepsilon}(1) \, \chi^{-1}((x)) \, x^n \, LF_{\alpha \mathbf{b}}^{(n)}(x\rho_{\mathbf{g}} + \beta^{-1}\varepsilon + P) .$$

Nous allons utiliser le lemme facile:

**3.7.3. LEMME. —** Deux éléments  $\mathbf{b}$  et  $\mathbf{b}'$  de  $\mathcal{R}_1$  donnent des nombres  $\beta$  et  $\beta'$  de  $1 + \Lambda^{(0)}$  dont les classes dans  $R_{\Lambda}^*/R_{\Lambda}^* \cap R$  sont distinctes.  $\square$

Supposons que  $\mathcal{M}'(\chi)$  soit infini : d'après 3.5.3, l'ensemble  $W$  des points de  $\Lambda^{\infty}$ -torsion  $w$  tels que

$$\sum \chi^{-1}(\mathbf{b}) \, G_{\mathbf{b}}(\beta^{-1}w) \equiv 0 \pmod{\underline{p}}$$

---

$\dagger$  on notera que  $K_{\Lambda^{\infty}} \cap H_{\mathfrak{g}\Lambda^{(0)}} = K_{\Lambda^{\infty}} \cap H_{\Lambda^{(0)}} = K_{\Lambda^{\infty}} \cap H$ .

est infini. D'après 2.3, et 3.7.3, toutes les fonctions  $G_b$  se réduisent modulo  $\bar{p}$  en des constantes. Or ceci est absurde, comme on le constate en calculant explicitement le diviseur polaire de  $G_b$ .  $\square$

### Bibliographie

- [F] FRIEDMAN E. — *Ideal class group in basic  $\mathbf{Z}_{p_1} \times \dots \times \mathbf{Z}_{p_s}$ -extensions of abelian number fields*, Invent. Math., **65** (1982), 425-440.
- [FW] FERRERO B. ET WASHINGTON L. — *The Iwasawa invariant vanishes for abelian number fields*, Ann. of Math., **109** (1979), 377-395.
- [Gi1] GILLARD R. — *Séries d'Eisenstein et critère de Kummer*, Sémin. Th. nombres, Paris, 1981-1982, p. 59-72, Birkhäuser: Boston-Basel-Stuttgart, 1983.
- [Gi2] GILLARD R. — *Fonctions  $L$   $p$ -adiques des corps quadratiques...*, J. reine angew. Math., **328** (1985), 76-91.
- [Gi3] GILLARD R. — *Croissance du nombre de classes dans des  $\mathbf{Z}_l$  extensions liées aux corps quadratiques imaginaires*. A paraître probablement aux Math. Annalen, 1987.
- [GR] GILLARD R. ET ROBERT G. — *Groupes d'unités elliptiques*, Bull. Soc. Math. France, **107** (1979), 305-317.
- [Gr] GRAS G. — *Groupe de Galois de la  $p$ -extension abélienne  $p$ -ramifiée maximale d'un corps de nombres*, J. reine angew. math., **333** (1982), 86-132.
- [I1] IWASAWA K. — *On the  $\mu$  invariant of  $\mathbf{Z}_l$ -extensions in Number Theory, algebraic geometry and commutative algebra*, p.1-11, Kinokuniya, Tokyo, 1973.
- [I2] IWASAWA K. — *On  $\mathbf{Z}_l$ -extensions of algebraic number fields*, ann. of Math., **98** (1973), 246-326.
- [K] KATZ N. — *Divisibilities, congruences and Cartier duality*, J. Fac Soc. Univ. Tokyo, **28** (1982), 667-678.
- [R1] ROBERT G. — *Unités elliptiques*, Bull. Soc. Math. France mém., **36** (1973), 77 p.
- [R2] ROBERT G. — *Nombres de Hurwitz et unités elliptiques*, Ann. Sc. Ec. Norm. Sup., **11** (1978), 297-389.
- [S1] SINNOTT W. — *On the  $\mu$ -invariant of the  $\Gamma$ -transform of a rational function*, Invent. Math., **75** (1984), 273-282.
- [S2] SINNOTT W. — *On a theorem of L. Washington*. Exposé aux journées arithmétiques de Besançon, 1985.
- [W1] WASHINGTON L. — *The non  $p$ -part of the class number in a cyclotomic  $\mathbf{Z}_p$ -extension*, Invent. Math., **49** (1978), 87-97.
- [W2] WASHINGTON L. — *Introduction to Cyclotomic fields*, Graduate text in Math., Springer Verlag, New-York, 1982.

Université de Grenoble I

**Institut Fourier**

Laboratoire de Mathématiques  
associé au CNRS

BP 74  
38402 Saint Martin d'Hères  
France